CHAPTER - 7

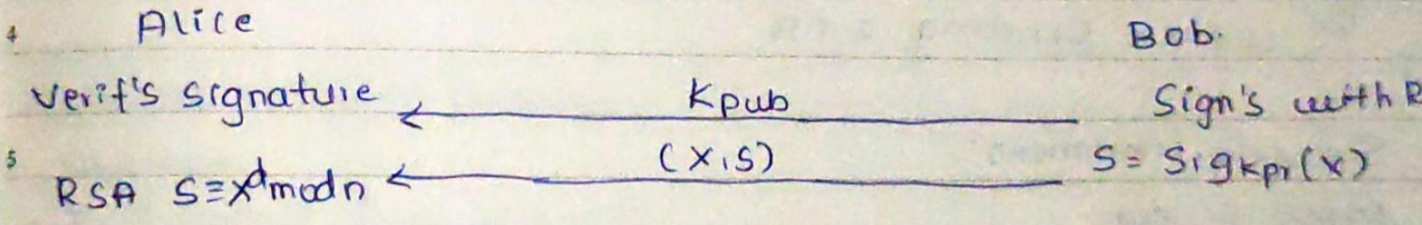
HASH FUNCTIONS.

- Hash function are an important cryptographic primitive and are widely used in protocols.

- They compute a digest of a message which is:- short fixed length bit-string.

- Hash function are auxiliary function in Cryptography, they are used for signatures, MAC's, Key derivation, RNG's.

Motivation Digital Signature



- The problem is X is restricted in length, n = 2048 bits
- 256 bytes most pdf's are longer

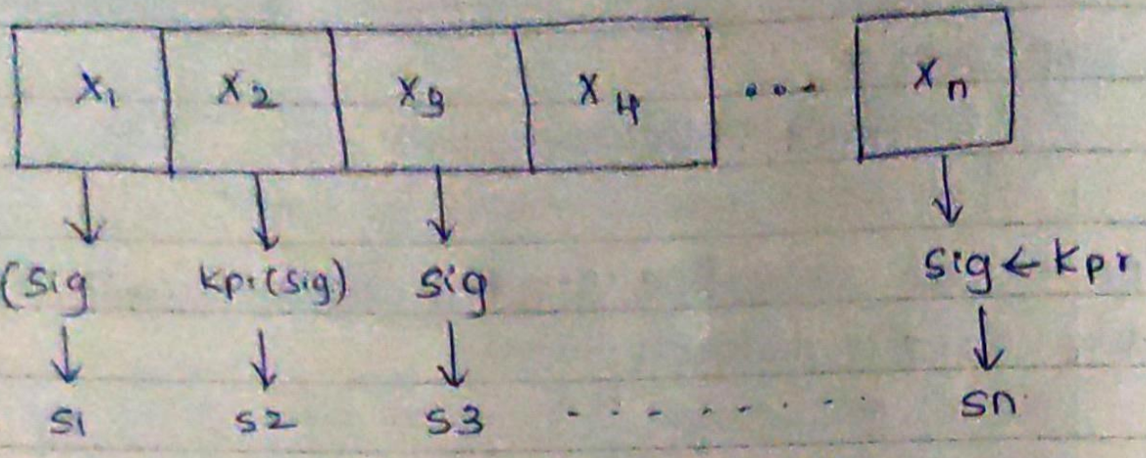
Problem:- X is restricted in length |x| < 256B.

So if you have 1KB file, we would have to chop the message and individually sign it

"It is a natural phenomenon of god that those who help others, god always helps them and bless them with growth and prosperity."

APR 17 2020 FRIDAY

Wk 16 (108-258)



This is Stupid, why?

High computational load:- DS are based on computationally intensive asymmetric operations. A single operation consumes a small amount of time, the signature of large message takes too long.

And verifier has to also verify message which takes time.

Doubles the message overhead since we are sending both message and signature. So 1mb file requires a 1mB signature So we are Sending 2mB

Security Limitations:-

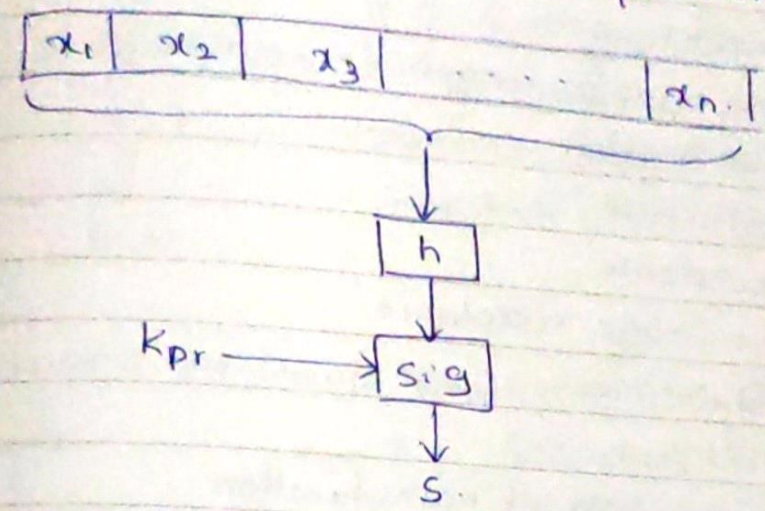
Most Serious:

Attempt to sign a long message by signing a sequence of message blocks individually.

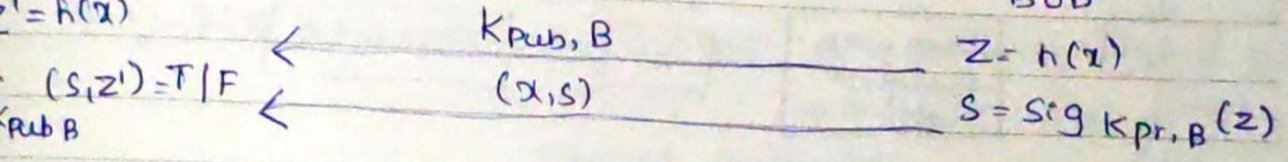
The attacker Oscar, could remove individual messages and the corresponding signatures or he would re-order messages and signatures or make new ones.

"Important is the kind feeling for all the people and animals, then you doesn't need any command from anyone, and you will do the best work you can."

what do we do? use hash functions.



Basic Protocol for Digital signature with hash functions



- we are not using message anymore
- Z is called "fingerprint of x" or a "message digest"

"A human nature can't be justified with your words but with your work, and is best judged when you do something for others and that too without exchange of any favour."

APR 19 2020 SUNDAY

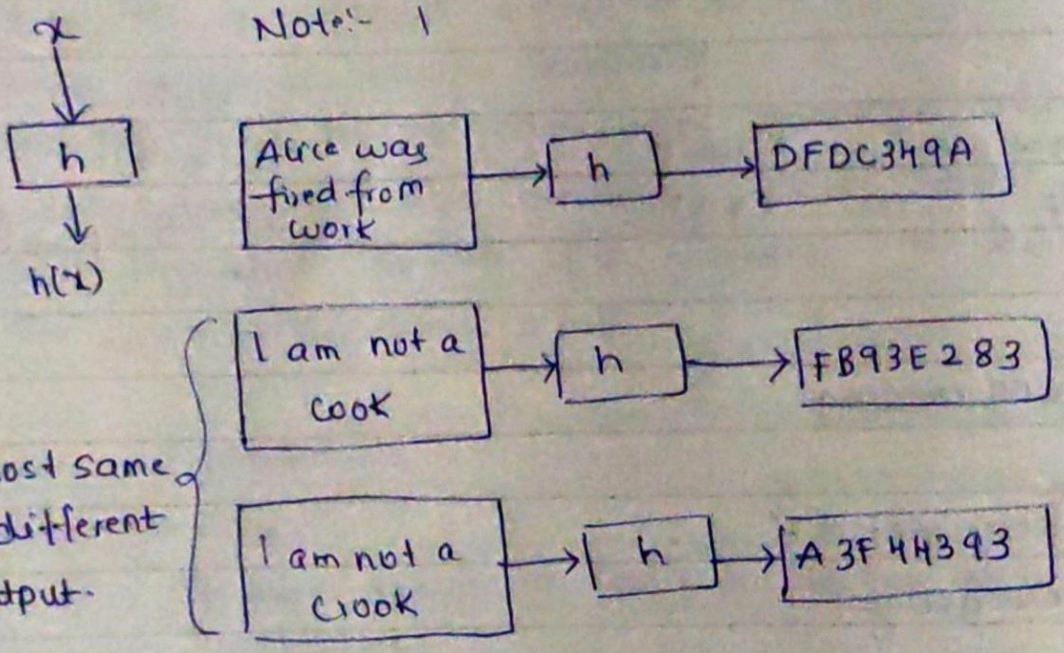
Wk 16 (110-256)

Requirements

1) Arbitrary input length
2) Fixed, short, output length (output length is same irrespective of input length)
3) Should be efficient
4) Preimage Resistance
5) Second pre-image resistance
6) Collision Resistance

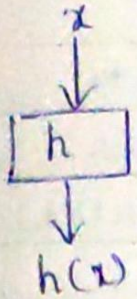
- Last three are about security of hash function.

Note:- 1



"When you risk your own life for the sake of others and that too an animal, that means you are the person with the heart of gold."

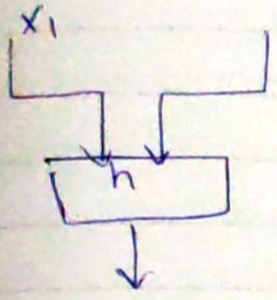
Pre-Image Resistance



If I give you $h(x)$ it should be impossible to go back

Protects you against an attacker who has $h(x)$ but trying to find x.

Second Pre-Image Resistance.



Essential that two different messages do not hash to the same value.

Oscar cannot find x_2 if he knows x_1

2nd pre image attack.

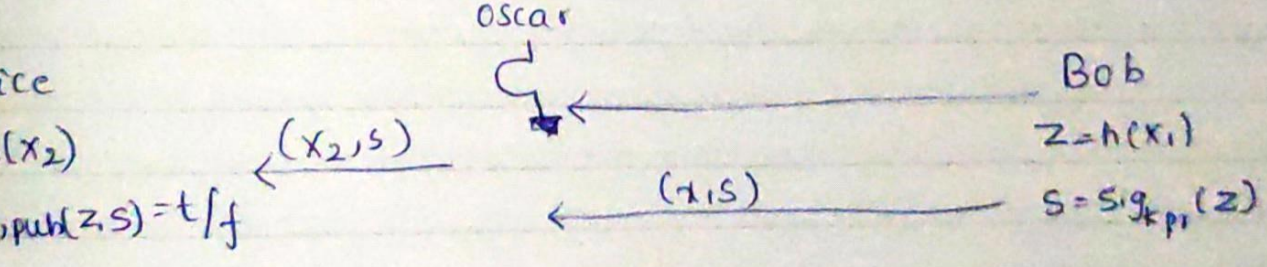
Ass Bob is sending a message to his bank

Assume x_1 = "Transfer 10 rupee's into Oscars account".

Oscar writeups:

x_2 = "Transfer 100,000 rupee's into Oscar's account.

and $h(x_1) = h(x_2) = z$

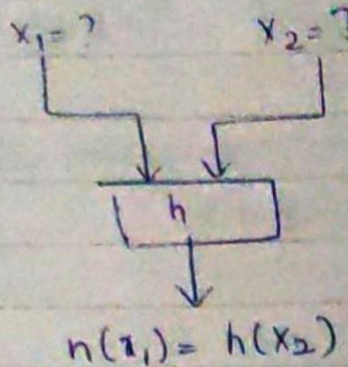


"Accept gifts with your heart and see other's emotions behind it, irrespective of the value and price tags of the presents."

APR 21 2020 TUESDAY

Wk 17 (112-254)

6) Collision Resistance



computationally infeasible to find two different inputs $x_1 \neq x_2$ with $h(x_1) = h(x_2)$

"Helping other people is a good human nature, but keeping a soft corner for animals is an example of humanity and a great deed ."